

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: USING A COMMUNICATION PROTOCOL TO
PROVIDE SECURITY SERVICES

INVENTOR: KELAN C. SILVESTER

Express Mail No. EL911616901US

Date: OCTOBER 10, 2001

USING A COMMUNICATION PROTOCOL TO PROVIDE SECURITY SERVICES

Background

This invention relates generally to techniques for preventing the theft of any of a variety of devices.

5 A variety of portable devices are subject to theft. Common examples are laptop computers, automotive electronics, desktop computers, home entertainment equipment, such as televisions, and a variety of other items. Generally, any theft deterrent that results in
10 greater inconvenience to the user often goes unused.

A variety of locks and other security devices are available for computers, but generally, relatively few people use these security devices. It is believed that the lack of utilization of these devices is not the result of
15 the lack of sufficient need to do so, but arises from the inconvenience involved in applying the security device.

Thus, there is a need for a security system that deters theft while reducing the amount of user involvement necessitated by the security system.

20 Brief Description of the Drawings

Figure 1 is a block depiction of one embodiment of the present invention;

Figure 2 is a flow chart for software in accordance with one embodiment of the present invention;

Figure 3 is a flow chart for software in accordance with one embodiment of the present invention;

Figure 4 is a schematic depiction of another embodiment of the present invention;

5 Figure 5 is a schematic depiction of still another embodiment of the present invention;

Figure 6 is a schematic depiction of yet another embodiment of the present invention; and

10 Figure 7 is a schematic depiction of still another embodiment of the present invention.

Detailed Description

Referring to Figure 1, a radio frequency protected device 14 may be coupled through a radio frequency protocol to a short-range radio frequency base station 12. The base station 12 may in turn be coupled to a system 32, which is
15 necessary for the operation of the protected device 14. The protected device 14 may be any of a variety of devices subject to theft including an automotive radio, a personal computer, a laptop computer, home electronics, a weapon, or
20 a cash register, to mention a few examples. The radio frequency protocol between the protected device 14 and the base station 12 may be any of a variety of relatively short-range (e.g., 10 meters) protocols including the Bluetooth Protocol (Specification of the Bluetooth System, Version 1.1, February 22, 2001).
25

Alternatively, longer range protocols may be used if it is acceptable to allow the protected device 14 to be operated in a wider area. For example, IEEE 802.11 wireless local area network has a range of 100 meters. See
5 IEEE Standard 802.11 available from the Institute of Electrical and Electronics Engineers, New York, New York.

The protected device 14 may include a controller 26 coupled to a storage device 28. In one embodiment, the storage device 28 may be a flash memory. The storage
10 device 28 may store software 30. A radio frequency interface 24 facilitates communications between the device 14 and the base station 12.

The base station 12 likewise includes a controller 18 coupled to an interface 16 and a storage device 20. The
15 storage device 20 may also be a flash memory, in one embodiment. The storage device 20 stores the software 22.

The controller 18 facilitates communications between the device 14 and the system 32 in one embodiment. In other words, the base station 12 enables communications
20 between the device 14 and components, devices or systems that are necessary for full operation of the device 14. For example, in connection with a protected device 14 that is a laptop computer, the short-range radio frequency base station 12 may provide the link to an electrical system.
25 Without the correct communication with the base station 12 through the radio frequency protocol, electrical power

would not be supplied to the protected device 14, as one example. As another example, the base station 12 may only allow a user to access stored data after being properly authenticated through the wireless protocol. As still
5 another example, the base station 12 may prevent booting unless the user is properly authenticated. Alternatively, the base station 12 may allow a limited boot, for example, sufficient to send a wireless message indicating an unauthorized user is attempting to use the system.

10 As a result, the proper establishment of radio frequency communications between the device 14 and the base station 12 is essential to the ability to use the device 14. The device 14 can not be effectively used without likewise obtaining the base station 12. The base station
15 12 may be secured in a fashion that makes it more difficult to remove. In some embodiments, one base station 12 may secure a number of protected devices 14. Thus, in one example, a laptop computer may be the protected device 14 and the base station 12 may be secured to a building.

20 If the protected device 14 is moved outside the range of the base station 12, it may no longer be operable in some embodiments. Thus, the system 32 may be the electrical system that provides power to the device 14 as one example. Only when the proper radio frequency (RF)
25 protocol is authenticated is the system 32 notified by the

base station 12 to provide essential services for the use of the protected device 14.

Referring to Figure 2, the software 22 in the base station 12 receives a handshake signal from a proximate wireless device, as indicated in block 32. The proximate wireless device may be an appropriate, authorized RF protected device 14. Upon receiving the handshake signal from the proximate wireless device, the base station 12 may request an identifier, as indicated in block 34. In block 10 36 an identifier is received from the proximate device. If the identifier is authenticated by the base station 12, as indicated in diamond 38, communication or operation with the system 32 may be allowed, as indicated in block 40, enabling the device 14 to be utilized. Otherwise, the 15 device 14 may not be utilized or communications may be prohibited, as indicated in block 42.

In accordance with an embodiment in which the radio frequency protocol between the base station 12 and the device 14 is the Bluetooth Protocol, the device 14 may 20 automatically implement the inquiry mode. In the inquiry mode, the device 14 attempts to determine what access points are within range. In-range devices, such as the base station 12, respond with their addresses and the device 14 selects one of the responding devices with which 25 to communicate. To establish communications, a paging mode is implemented wherein the devices 12 and 14 synchronize

with one another. Then, the devices undergo the service discovery mode wherein the device 14 discovers what services are available from the base station 12. Thereafter, communication may be implemented followed by
5 the authentication protocol described previously.

Referring to Figure 3, the software 30 on the protected device generates a handshake signal, as indicated in block 48. When it receives a response, as determined in diamond 50, from the base station 12, it provides the
10 requested identifier, as indicated in block 52.

Embodiments of the present invention are amenable to a wide variety of applications. For example, in Figure 4, the RF protected device 14 may be a car radio 14a. The radio 14a may communicate with a short-range RF base
15 station 12 secured within a vehicle. For example, the base station 12 may be inside the dashboard or in a relatively difficult to access location. The short-range RF base station 12 may only allow communication between the radio 14a and the electrical system 32a when the radio 14a is
20 properly authenticated. For example, electrical communication may be switched off until such time as proper authentication is received from the incoming car radio 14a. Thus, if one were to steal the car radio 14a, it would not work in any other vehicle without the base station 12.
25 This would deter theft, increasing the value of the car radio 14a. As another example, the radio 14a may generate

static or obnoxiously altered sounds if proper authentication is not achieved.

Referring to Figure 5, an embodiment is depicted in which a personal computer 14b is the RF protected device 14. In this case, the personal computer 14b may communicate with a short-range RF base station 12 that may be concealed, for example, within the user's desk. For example, the base station 12 may control the power to the personal computer 14b. In one embodiment, the base station 12 may communicate wirelessly with an appropriate switch within the personal computer 14b to allow the computer to receive power.

Referring to Figure 6, a laptop computer 14c may communicate with a short-range compact RF base station 12a that may be in the form of a key fob in one embodiment. The computer 14c is only operable when the base station 12a, carried by the user, is in range. Again, the base station 12a may provide selective operation of a power control 32b to allow the laptop computer 14c to be operated.

As still another example, referring to Figure 7, a home electronics device 14d may be a television, a stereo, or a digital versatile disk player. The device 14d may communicate with a base station 12 that provides selective control through access to the power control module 32b. Unless the electronics device 14d is properly

authenticated, the base station 12 does not permit power to be applied to the home electronics device 14d. In such case, if the thief steals the device 14d, the device 14d may be inoperable without the base station 12 (that would not be available to the thief). For example, the base station 12 may be hidden within the walls of the user's home or otherwise concealed.

While the present invention has been described with respect to a limited number of embodiments, those skilled in the art will appreciate numerous modifications and variations therefrom. It is intended that the appended claims cover all such modifications and variations as fall within the true spirit and scope of this present invention.

What is claimed is: